**LITERATURE REVIEW**

1. **A Comprehensive Review of ML-Based Intrusion Detection in IoMT**

ML-based hybrid IDS models have shown superior performance in meeting the low-latency and interpretability needs of resource-constrained, high-risk IoMT (Internet of Medical Things) environments [[1]](https://link.springer.com/article/10.1007/s10462-024-11101-w?utm_source=chatgpt.com#citeas).

* Identifies critical gaps between lab-developed IDS models and real-world IoMT deployment, particularly in handling dynamic medical data and device constraints, such as battery life, limited memory.
* Confirms ML/DL models such as SVM, LSTM, and CNN outperform rule-based approaches in detecting diverse threats in real time, with better generalisation and adaptability.
* Stresses importance of explainability and low false positive rates as top criteria for clinical deployment, due to the high stakes in medical decisions.
* Note lack of labelled, real-world datasets as a core barrier, most existing models rely on outdated or synthetic data, affecting model reliability.
* Recommends hybrid architectures, such as LSTM and Autoencoder, to handle evolving threats and reduce overfitting on limited datasets.
* Highlights the need for context-aware IDS that adapt to the unique operating conditions and risk profiles of various IoMT devices.

1. **AI-Driven Intrusion Detection Systems for IoT: A Survey**

Federated and unsupervised learning techniques are emerging as scalable, privacy-preserving approaches for anomaly detection in sensitive health IoT systems [[2]](https://thesai.org/Downloads/Volume16No6/Paper_47-AI_Driven_Intrusion_Detection_Systems.pdf?utm_source=chatgpt.com).

* Deep learning methods, such as CNN, RNN, LSTM, are shown to detect complex, multi-stage attacks in IoT networks more effectively than classical models.
* Autoencoders excel at identifying zero-day threats, leveraging their unsupervised training to flag deviations from normal behaviour, especially useful when labels are scarce.
* Transfer learning is highlighted as a workaround for small or domain-specific datasets, enabling IDS reuse across different IoT environments with minimal retraining.
* Federated learning is proposed for privacy-preserving IDS, enabling distributed model training without exposing raw patient data, which is ideal for healthcare IoT.
* Model complexity vs. inference speed trade-offs are discussed, particularly for real-time detection on wearables and edge gateways.
* Combining federated, unsupervised, and lightweight models is identified as a promising strategy for future IDS in IoMT.

1. **Security Threats in IoMT and the Role of AI-Based IDS**

Context-sensitive, ethically aligned AI models such as GNN-based IDS improve trust and detection performance in complex IoMT ecosystems [[3]](https://www.mdpi.com/2673-2688/4/3/28).

* Enumerates dominant IoMT threats, including DoS, spoofing, adversarial attacks, and privacy breaches from insecure communications.
* Context-aware IDS are advocated, adjusting thresholds or detection logic based on device behaviour, application type, or user health state.
* Graph Neural Networks (GNNs) are recommended to detect anomalous device interactions across interconnected topologies, especially valuable in hospital or home-health networks.
* Emphasises ethical AI principles, including fairness, transparency, and accountability in IDS models, aligning with medical data governance.
* Stresses need for cloud–edge collaboration, where initial analysis happens at the edge, such as low latency, and deeper threat analysis occurs in the cloud, such as greater processing power.

**REFERENCE**

[1] A. Naghib, F. S. Gharehchopogh, and A. Zamanifar, “A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities,” Artif Intell Rev, vol. 58, no. 4, p. 114, Jan. 2025, doi: 10.1007/s10462-024-11101-w.

[2] M. S. Nawaz, M. A. Raza, B. Raza, M. Ahmad, and F. Syed, “AI-Driven Intrusion Detection Systems for Securing IoT Healthcare Networks,” International Journal of Advanced Computer Science and Applications, vol. 16, no. 6, 2025.

[3] R. Lazzarini, H. Tianfield, and V. Charissis, “Federated Learning for IoT Intrusion Detection.” Accessed: Jul. 25, 2025. [Online]. Available: https://www.mdpi.com/2673-2688/4/3/28?utm\_source=chatgpt.com